Cyberdefense

Swift

Customer Security Program (CSP) Assessment & Consulting

The challenges of compliance

Swift introduced a security program named the Swift Customer Security Program (CSP) considering increasing cyber-attacks. The core component of CSP is the Customer Security Controls Framework (CSCF), which describes a set of mandatory and advisory security controls for Swift users.

Mandatory security controls establish a security baseline for the entire Swift community and must be implemented by all users on their local Swift infrastructure. Swift has prioritized these mandatory controls to set realistic goals for near-term, tangible security gain and risk reduction.

Advisory controls, on the other hand, are based on best practices that Swift recommends implementing. They provide additional security measures that, while not mandatory, are highly beneficial. It's important to note that over time, as the threat landscape evolves, some advisory controls may transition to become mandatory, further enhancing the security of your operations.

Every organization using Swift must confirm effective compliance with the mandatory security controls no later than 31 December each year. An independent assessment is a prerequisite for attestation, to enhance the integrity, consistency, and accuracy of attestations.

A reliable partner since the very beginning

Orange Cyberdefense has been conducting CSP assessments and assisting our clients with their attestation requirements since the framework's inception. Our CSP assessments are conducted by security experts who value not only compliance but are also passionate contributors to a safer financial ecosystem.

Our approach and methodology

1. Preparation & Collection

As a start, a kick-off session is organized to launch the assessment and identify the client. Participants, documentation needed, and the project plan.

2. Understanding & Assessment

During this phase, we aim to understand your IT and Swift environment, its structure, and the security measures in place. This understanding is facilitated through workshops, which are part of the design phase. In these workshops, we verify if your controls and security measures, as designed, align with the operational requirements.

3. Testing & Analyzing

This part is a test of effectiveness, where we ensure that the controls and security measures described are effectively in place, without exception, and delivering the expected results.

4. Reporting

At the end of the assessment, we prepare a full report under the Swift CSCF requirements, including a confirmation letter required for attestation.

Find out more about our assessments:
orangecyberdefense.com/za/offering/identify

Streamline: Create a structure that meets CSP requirements, consistent with your operations and systems already in place.

Secure: Use expertise in security and financial services to protect your core banking systems. With specific support, deploy the necessary and sufficient measures to manage your risks.

Identify the projects to be carried out and establish a pragmatic schedule.

Compliance: Get ready to meet growing compliance demands and confidently present your attestation.

Challenges

- Staying on top of all compliance requirements is a hassle
- Compliance requirements may change due to the evolving threat landscape
- Traditional compliance assessments lack context in terms of practical security best practice

When should you consider it?

- If you require insight from security experts that goes beyond a traditional compliance assessment
- If you require an assessment for CSP compliance If you want to prepare for an assessment

What do we do?

- We provide expert advice on setting up your architecture for both security and compliance
- Based on our unmatched threat intelligence, we help
- you prioritize strategic security efforts
- We offer additional services to meet the requirements of the CSP framework, including Swift-specific pentests, Incident Response table-top simulations, etc.

What will you get?

- A walk-through to compliance: workshops to define
- project scope and planning
- Strategic recommendations for improvements are available as an optional value-add.
- Testing the implemented measures for effectiveness
- Assessment report in line with the Swift requirements
- Strategic recommendations for improvements is available as an optional value-add

For more information, check
https://www.orangecyberdefense.com/global/

100 Galleria Parkway, Suite 300
Atlanta, GA 30339

sales.desk@orange.com
+1 (678) 346-3003